AusCERT

Australia's National Computer Emergency Response Team

Senate Select Committee on the National Broadband Network

Background

A Senate Select Committee has commenced an inquiry into the National Broadband Network (NBN). AusCERT was invited to provide a submission to this Committee inquiry.

In making this submission, AusCERT has addressed some of the committee's Terms of Reference.

Executive summary

The high level of cybercrime targeting Australian interests has the potential to seriously harm the Australian economy and undermine confidence in the online economy. Cybercrime already poses a significant problem for insecure Australian networks and computers and attacks that harm Australian Internet users are commonplace.

It is assessed that the NBN has the potential to be a force-multiplier for cybercrime attacks directed at Australian networks and information systems because cyber criminals are attracted to attack, compromise and use systems with high speed broadband access. Compromised computer systems with high speed access significantly increase the impact and effectiveness of most internet based attacks.

At present, without significant changes to the way e-security is managed across the entire Australian community, the NBN and the online information and service economy it will support, will simply provide greater opportunity for (predominantly overseas based) cyber criminals to prosper at our expense with relative impunity. Indeed, the harm to our citizens, communities and economies, could be far more reaching and serious than many realise as levels of fraud associated with identity theft continues to grow.

If current attitudes and approaches to dealing with the cybercrime problem by government and industry do not significantly change and improve, then gains in building an online economy, through the provision of new businesses, services and the physical infrastructure, such as the NBN for the benefit to our citizens, communities and economies will be seriously undermined.

The issue for the committee is whether the potential force-multiplier effects of cybercrime brought about by the NBN will outweigh or seriously harm or reduce the capacity of the NBN to facilitate national productivity, economic growth, etc?

About AusCERT

AusCERT[1] is Australia's national computer emergency response team (CERT). [2]

[1] www.auscert.org.au

AusCERT, which was formally established in 1993, is an independent, self-funded, not-for-profit, non-government organisation, based at the University of Queensland. AusCERT employs around 20 information and cyber security experts.

As the national CERT for Australia, AusCERT is the primary point of contact for the provision of advice about computer network threats and vulnerabilities in Australia and provides an incident response service for Australian networks for cyber attacks emanating from both overseas and from within Australia.

Due to AusCERT's substantial experience monitoring, analysing and responding to cyber attacks in Australia and from abroad for over 15 years, AusCERT has a sound understanding of e-security risks more generally. This understanding extends to a strong technical understanding of :

- how cyber criminals are able to defeat the security of computer systems, attack computer systems, take control of them and steal data from them;
- how the underlying infrastructure is vulnerable to attack and compromise and the limitations of various security related technologies and mechanisms which are put in place in an attempt to prevent or detect attacks.

Terms of Reference

AusCERT has only addressed specific aspects of the terms of reference, which are most relevant to our area of expertise/interest. It is noted that:

- the implications for cyber security for Australia as a result of the roll out of the NBN; and
- the security of the NBN itself

are not specifically part of the terms of reference, which is concerning as it may mean that important cyber security issues are not addressed during the design, planning and implementation of the NBN. Attempting to retrofit security to the NBN would be disastrous.

Therefore, AusCERT will seek to identify various security related implications associated with the NBN in terms of its impact on economic factors, inter alia, which is part of the terms of reference.

[2] In May 2009, the Attorney-General's Department advised AusCERT that the Australian government would take over the role of national CERT from AusCERT and that it would contract AusCERT to provide some services to the Department in support of this role. As the new national CERT is not yet established, AusCERT continues to perform the role of national CERT on a self-funded basis.

The terms of references invites comments on:

1(b) The implications of the NBN for consumers and taxpayers in terms of [...]

iii likely consequences for national productivity, investment, economic growth, cost of living and social capital.

The volume and level of cyber attacks directed at Australian Internet users, government systems and business networks is likely to significantly increase with the roll out of the NBN. This is likely to have an adverse impact on national productivity, investment, economic growth and cost of living and social capital.

In the same way that the NBN is likely to be a positive enabler for economic growth, innovation and investment, in the context of cybercrime, the NBN will also be an enabler, indeed a force-multiplier, for cybercrime. As noted in previous papers by AusCERT relating to cyber attacks and cybercrime, cybercrime is already a serious problem in Australia and, as a society, e-security risks are generally not being well managed. [3]

The issue for the Senate Select Committee is whether the force-multiplier effects of cybercrime brought about by the NBN will outweigh or significantly undermine the capacity of the NBN to facilitate national productivity, economic growth etc? AusCERT assesses that unless substantial progress is made to better manage e-security risks across government and industry than presently occurs, then there is a real risk that the NBN will provide greater appeal to attack computers and networks in Australia in support of illicit financial gain.

Why is the NBN likely to be a force-multiplier for cybercrime?

AusCERT has actively been monitoring, responding to, and mitigating a range of cyber attacks motivated by illicit financial gain since 2003 which target online services and systems. The growth and sophistication of attacks has been constant since then.

It is generally recognised that the level of malicious Internet activity and cybercrime increases in proportion to the availability of, high speed broadband services.[4] [5] This is because cybercriminals are attracted to compromise and control computers on networks with powerful broadband capabilities because this provides them with the greatest versatility and reliability in how they may use their compromised "bot" hosts.

Well known F-Secure security expert, Mikko Hypponen, said that:

> *We have seen malware which when it infects a PC, the first thing it does is connect to a university file server to download a gigabyte size Linux installation DVD package to*

[3] See references at end.

[4] OECD, Malicious Software (Malware) – A Security Threat to the Internet Economy. http://www.oecd.org/dataoecd/53/34/40724457.pdf, page 26

[5] CERT/CC (2005), Botnets a vehicle for online crime, www.cert.org/archive/pdf/Botnets.pdf

> *clock the speed. If it is too slow it just rejects the PC. [Hackers] have so many machines at their disposal they can choose to be picky.*[6]

Companies that monitor distributed denial of service attacks (such as Prolexic and Arbor) report an increase in capacity of DDOS attacks which is attributed to bots that have high speed broadband access. [7] This is not surprising but demonstrates the appeal of criminals compromising computers with high speed access and using these for attacks. Bots within Australia could be used for DDOS attacks against targets abroad, inter alia, or DDOS attacks locally.

When the government's new fibre to the premise, national broadband network (NBN) is built, the level of interest in targeting Australian computers is likely to significantly increase, as the NBN will be in a position to support greater traffic volumes/activity associated with cybercrime.

Botnets, like the malware used to create botnets, *inter alia*, are a vehicle to facilitate online crime.[8] A bot is a compromised computer; a botnet is a set of compromised computers, often many hundreds or thousands, in control of an attacker/criminal and are used to support various additional cybercrimes, beyond the compromise of the computers themselves. Botnets are used for DDOS attacks and to support online identity theft, and a range of other cybercrimes.

For example, recent analysis of a Torpig botnet revealed that within a space of just 10 days, criminals used this malware to attack and compromise 180,000 computers around the world and captured 70GB of compromised sensitive information from these computers and their users. Moreover, a further 1.2 million[9] Torpig compromised computers were observed contacting the command and control server. [10] Torpig, which has been around since 2006, is just one of many serious types of malware that have been targeting Australian computers since around 2004 for illicit financial gain. Despite it being around for some years, attackers constantly modify the malware to produce new variants that are undetectable to many anti-virus products at the time of release.

How does the proposed NBN compare to existing broadband speeds elsewhere and why this is relevant to cybercrime?

Cybercriminals are mindful of the processing capabilities of the computer itself and the Internet bandwidth access of the computer itself.

[6] http://www.computerworld.com.au/article/310538/nbn_accelerate_botnet_attacks?fp=39&fpid=25938

[7] https://www.linx.net/files/hotlinx/hotlinx-17.pdf, page 3

[8] Ibid. CERT/CC, (2005)
Ibid., OECD
AusCERT, (2006) Haxdoor - anatomy of an online identity theft attack, http://www.auscert.org.au/7069

[9] The authors acknowledge this figure may be inflated where it is based on counting unique IP addresses alone, which may be inflated due to dynamic IP address allocation practices. Generally bots will assign a unique identification number which is a more reliable method of counting infected computers as part of a botnet.

[10] http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf

Indeed, the speed of the NBN proposed (ie 90% of premises will have 100 Mbps) will substantially leapfrog average speeds for most other countries in the world which currently have high levels of high speed broadband penetration. [11] Surpassing the broadband speeds in other countries may have the unintended consequence of making Australia a preferred destination by criminals to host cyber attacks directed both at Australian interests and those abroad.

For example, while Japan and Korea which are considered the most advanced countries in terms of broadband speeds where they can offer fibre optic speeds of up to 1,000 Mbps (or approximately 1 Gbps),[12] on average speeds are only around 17 Mbps.[13] Also the fastest download speeds for OECD countries that have fibre-to-the-x (FTTx), where x is the node (street) or premise, is around 65 Mbps.[14]

The Australian NBN plan to provide an average and median of around 100 Mbps could shift the current dynamics of cyber attack, making Australian computers an even more attractive target for hosting botnets that facilitate cybercrime, compared to much lower averages (at least currently) elsewhere. It is for this reason that the NBN is assessed to be a potential force-multiplier for existing cybercrime levels in Australia.

Opportunity exists to build better security into the network layer

Traditionally, cyber security has been pushed to the end points with the end points having to bear the greatest level of the cyber security burden. An end point can be a home user computer connected to the Internet via their ISP, business web servers, mail servers, domain name servers or a business or organisational network. End points must defend themselves from various forms of attack and compromise, from denial of service attacks, from malware, from theft of data, etc. The security of each end point will vary according to who owns and operates these systems and how they are managed from a security perspective.

A key concern with the NBN, as with the existing telecommunication backbone network, is that there will be little or no security built into the NBN backbone network. Rather, as currently applies, it will be increasingly important for the end points to bear the major responsibility and burden for security measures, which is already resource intensive, complex and challenging.

The ISP and carrier networks which route IP traffic in Australia have generally not played a significant role in adopting measures which would help to reduce the level and nature of attacks end points experience. The reality is that some aspects of security are best handled by the end points, but there are other areas where the carrier networks is able to implement greater levels of security than presently exists, and reduce some types of malicious activity directed at end points.

[11] http://websiteoptimization.com/bw/

[12] OECD, www.oecd.org/dataoecd/11/35/39575199.xls

[13] That is the average for OECD countries. OECD, www.oecd.org/dataoecd/10/53/39575086.xls

[14] OECD, www.oecd.org/dataoecd/10/54/39575095.xls

As the NBN implementation committee determines how it proposes to connect these premises to the (new or existing) backbone carrier networks, the implementation committee has the opportunity to mandate the adoption of technologies and strategies which support more secure network topologies and traffic routing and management.

For example, carriers and network operators have the capacity to implement the use of more secure protocols involved in the transfer of packets across the Internet. Use of existing security protocols widely within the ISP, telecommunications carrier networks, including for the NBN, would reduce the ability of criminals to conduct some types of cyber attacks and help reduce ensuing harm to the users of the NBN.

These could include adoption of DNSSEC,[15] IPSec (as part of IPv6)[16], SBGP[17], and other strategies deemed appropriate/beneficial, of which there are many others. It is not the purpose of this submission to identify all strategies which could be effective, but as an indication the Arbor Infrastructure Security Report refers to a number of strategies and processes, which if implemented at the ISP level would help reduce the already high security burden on end points.[18]

None of these strategies, by themselves or together are a panacea for the variety of cyber attacks that occur on the Internet directed against Australian internet users, however, in combination they will assist in reducing some types of attack and the volume of attacks and help reduce the security burden on end points.

The backbone architecture of the NBN and its relevance to cyber security for Australia

Currently, there is a lack of detail about the technical aspects of the NBN implementation, particularly at the cloud, backbone, carrier level. It is expected that part of the funding for the NBN will be to build new backbone architecture through a new carrier network and/or augment existing backbone architecture owned and operated by existing carriers.

It is likely that the backbone architecture will use Next Generation Networks (NGN) technologies, ie be capable of carrying heterogeneous data, voice and video traffic over a

[15] For further information about what DNSSEC is and helps prevent refer to http://www.dnssec.net/ DNSSEC is typically implemented to whole domain name spaces such as to an entire ccTLD or sub domain; eg, it could be applied to all domains within .au; or to sub domains of .au such as .gov.au or .com.au. The more widely deployed across the legitimate domain name space, the better.

[16] IPSec can be implemented as part of IPv4 or IPv6. IPv4 requires manual/optional implementation of IPSec protocols, whereas IPSec functionality is a mandatory feature of IPv6.

http://www.6deploy.org/e-learning/english/what_is_ipv6/

http://www.ipv6.org/

[17] http://www.ir.bbn.com/sbgp/

Six worst Internet routing attacks: http://www.networkworld.com/news/2009/011509-bgp-attacks.html

[18] Arbor, Worldwide Infrastructure Security Report, October 2008, http://www.arbornetworks.com/report, pages 16-24

homogenous IP network.[19] The use of NGN technologies is not restricted to any existing carrier but is a trend being adopted by carriers and network service providers worldwide.

The significance of this from a national cyber security perspective is that greater homogeneity reduces redundancy and exposes day to day and critical telecommunications traffic (including NBN traffic) to a greater variety of common TCP/IP[20] related threats. [21]

For example, in a next generation network, the mobile telephone and PSTN will converge with the IP network at various points. The redundancy provided by three separate types of voice networks/topologies (Voice over IP, PSTN network and mobile 3G/GSM networks) is reduced. These different networks may not disappear entirely but at least part of the network will depend on IP carriage and it will be these common areas of dependency that could also be a point of common failure due to accidents or cyber attacks.

For example, as a result of the widespread distributed denial of service (DDOS) attacks that were directed at Estonia networks in 2007, some outages of the mobile GSM network were experienced. It is assessed this was an indirect impact of the DDOS attack where GSM traffic converged with IP networks, which experienced increased levels of IP attack traffic.

The combination of both these technological changes to the digital landscape in Australia has the potential to significantly exacerbate the current threat environment and provide even more reason to implement and support a range of strategies to reduce e-security risks in Australia.

2. d. any regulations or legislation pertaining to the NBN

As outlined above, many aspects of the NBN will involve the provisioning of carrier backbone traffic. Carriers have the capacity to use processes, technologies and protocols which enhance the overall security of internet protocol (IP) traffic, which could reduce the burden (but not eliminate) on end points to protect themselves from cyber attack.

In Finland, which is regarded as "among the safest countries in the world with very low malware infection rates" it is estimated that about 1% of broadband users have a bot compromised computer.[22] According to leading Finnish security anti-virus vendor, F-Secure, ISPs in Finland actively police their networks and there are strong regulatory controls provided to authorities.[23] In all likelihood the low infection rates shows the benefit of greater effort and responsibility to improve network security by ISPs and carriers.

[19] This is often referred to as "triple play" – referring to the carriage and convergence of voice, video and data over an IP network.

[20] TCP/IP is a suite of many protocols used to route different traffic types over IP networks, including the Internet. While the protocols and traffic types vary they all use the common IP protocol at the network layer. (Mostly this is IPv4 but also potentially IPv6 – if changes are made to allow this to occur).

[21] Arbor, The Service Provider Challenge: Managing the Triple Threat to Triple-Play, page 2, http://www.arbornetworks.com/en/white-papers.html

[22] http://www.f-secure.com/en_EMEA/security/security-lab/latest-threats/security-threat-summaries/2008-4.html, Busy Botnets

[23] F-Secure, ibid.

Even in Japan which has already high bandwidth has implemented nation wide and effective approaches to detecting and removing botnets within Japan through its Cyber Clean Program.[24]

However, ISPs and carriers are not the only stakeholders which have the capacity to help prevent and reduce certain types of cybercrime. A poor level of security among many Australian web host providers/servers/applications make them vulnerable to attack and used, in turn, as a vector to attack the broader local population.

Common forms of attack involve compromising legitimate web sites to serve malware to the public intended for illicit financial gain. The government could, through regulation, improve the quality of web application/server security and domain name servers (inter alia) hosted in Australia to reduce the opportunity for this type of attack and at the same time ensure that personnel employed to develop and host web applications/servers/sites have cyber security qualifications.

The government has a responsibility to ensure that Australian hosted web sites/domains are securely constructed and maintained and do not pose a threat to users and their computers which connect to those web sites to view their content.

Similarly, Australian registries/registrars could follow a Code of Conduct adopting the APWG Best Practice Guide, which would reduce the number of domains registered for fraudulent/criminal purposes by Australian registrars and re-sellers as part of the gTLD or .au ccTLD namespace and improve the processes for timely deregistration of known fraudulent domains, registered by registrars and re-sellers in Australia.[25]

Conclusion

As demonstrated by the Finnish and Japan cases, access to high speed broadband access does not necessarily mean cybercrime will proliferate. The cases do suggest that a more intensive, focused, holistic approach to cyber-security across the community nationally can be critical to better managing (preventing and responding to) cybercrime.

The purpose of this submission is to highlight the importance of developing a more comprehensive approach to cybercrime prevention, detection and response across all stakeholders and network operators. This will be critical if the NBN is to provide positive rather than negative return on its investment and help – not hinder – the Australian economy, inter alia.

Maintaining the status quo in relation to existing cyber security approaches in Australia is not an option.

[24] https://www.ccc.go.jp/en_index.html
https://www.ccc.go.jp/en_report/200901/index.html
https://www.ccc.go.jp/en_report/h19ccc_en_report.pdf

[25] http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf

Further references about cyber attack and botnet activity

Symantec Global Internet Security – Trends for 2008, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

OECD, *Malicious software (malware): a security threat to the Internet economy*, http://www.oecd.org/dataoecd/53/34/40724457.pdf (2008)

UK House of Lords, Science and Technology Committee, *Personal Internet Security*, Volume I, http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf (2007)

Arbor, Worldwide Infrastructure Security Report, October 2008, http://www.arbornetworks.com/report

Shadowserver, (Botnet monitoring), http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCounts

Further papers by AusCERT relating to cyber attacks and cybercrime

AusCERT, *Managing Risk Associated with Online ID Theft for Government and Providers of e-Government Services*, http://www.auscert.org.au/5777 (2005)

AusCERT, *Haxdoor - Anatomy of an ID Theft Attack Using Malware,* http://www.auscert.org.au/7069 (2006)

AusCERT, Submission to the Australian Law Reform Commission, Review of the Privacy Act 1988, http://www.auscert.org.au/8510 (2008)

AusCERT, Submission to Attorney-General's e-Security Review, http://www.auscert.org.au/9771 (2008)

AusCERT, *Home Users Computer Security Survey 2008*, http://www.auscert.org.au/usersurvey

AusCERT, Submission to .auDA, Review of the .au domain name policy framework, http://www.auscert.org.au/8396 (2007)

AusCERT, Submission to ASIC, Electronic Funds Code of Conduct Review, http://www.auscert.org.au/7536 (2007)

AusCERT, Submission to .auDA, Review of the structure and operation of the .au Internet domain, http://www.auscert.org.au/7019 (2006)

AusCERT, Submission to DCITA, Review of the e-Security National Agenda, http://www.auscert.org.au/7037 (2006) (confidential and public submissions)

AusCERT, Submission to ACMA, Review of the Spam Act 2003, http://www.auscert.org.au/6200 (2006)